Nonbinary Quantum Stabilizer Codes

Alexei Ashikhmin * Emanuel Knill †

Abstract

We define and show how to construct nonbinary quantum stabilizer codes. Our approach is based on nonbinary error bases. It generalizes the relationship between selforthogonal codes over $\mathbf{F}_4$ and binary quantum codes to one between selforthogonal codes over $\mathbf{F}_{q^2}$ and q-ary quantum codes for any prime power q.

Index Terms — quantum stabilizer codes, nonbinary quantum codes, selforthogonal codes.

1 Introduction

Probably the most important class of binary quantum codes are quantum stabilizer codes. They play a role similar to the linear codes in classical coding theory. Quantum stabilizer codes have simple encoding algorithms, can be analyzed using classical coding theory, and yield methods for fault tolerant quantum computation. The first examples of quantum codes found by Shor [17], and Steane [19, 20] were quantum stabilizer codes. General quantum stabilizer codes were introduced by Gottesman [8] and Calderbank *et. al.* [6]. Later Calderbank *et. al.* [7] gave the now standard connection between quantum stabilizer codes and classical selforthogonal codes, which was used to construct a number of new good quantum codes.

While the theory of binary quantum stabilizer codes is now well developed, nonbinary codes have been relatively ignored. A connection between classical codes over $\mathbf{Z}_n$ and quantum codes is given in [10, 11]. The connection is based on a stabilizer construction derived from so-called nice error bases. Raines [15] obtained a number of results for p-ary (p prime) quantum stabilizer codes generalizing the $\mathbf{F}_4$ constructions for binary quantum codes.

Here we consider the problem of constructing p^m-ary quantum codes from classical selforthogonal codes over $\mathbf{F}_{p^{2m}}$. The notion of selforthogonality arises naturally from the error bases of [10, 11] and can be identified with that arising from a field-theoretically defined simplectic form. Good self-orthogonal codes with respect to this form have already been found by Bierbrauer and Edel [5], and our construction can be used to obtain associated quantum codes.

*Bell Laboratories, Lucent Technologies, 600 Mountain Ave., Rm.: 2C-180, Murray Hill, NJ 07974.

†Los Alamos National Laboratory Group CIC-3, Mail Stop B265, Los Alamos, NM 87545.

2 Basic Definitions

We start with the basic notions of classical and quantum coding theory. Denote by $\mathbf{F}_{p^m}$ the Galois field of p^m elements, where p is a prime number and m is an integer. Let $\alpha_1, \alpha_1, \ldots, \alpha_m$ denote the elements of a basis of $\mathbf{F}_{p^m}$ over $\mathbf{F}_p$. We fix a non-zero $\mathbf{F}_p$-linear functional $\mathrm{tr} : \mathbf{F}_{p^m} \to \mathbf{F}_p$ (called a *trace function*). Thus tr satisfies

$$\begin{aligned} tr(a+b) &= tr(a) + tr(b), \\ tr(\alpha a) &= \alpha tr(a), \end{aligned}$$

for all $a, b \in \mathbf{F}_{p^m}, \alpha \in \mathbf{F}_p$. Note that for $x \in \mathbf{F}_{p^m}$, $\mathrm{tr}_x(a) = \mathrm{tr}(xa)$ defines another trace function, and that all such functions can be obtained this way. The standard trace function is the one defined by viewing $\mathbf{F}_{p^m}$ as an extension of $\mathbf{F}_p$ and letting $\mathrm{tr}(a) = \sum_{i=0}^{m-1} a^{p^i}$, [14, Chapter 2.3].

Let t divide m. A classical p^t-linear code C over a field $\mathbf{F}_{p^m}$ of length n and size $(p^t)^k$, is a k dimensional p^t-linear subspace of the space $\mathbf{F}_{p^m}^n$. In other words, for any $\mathbf{a}, \mathbf{b}$ from C and any $\alpha, \beta \in \mathbf{F}_{p^t}$ the vector $\alpha\mathbf{a} + \beta\mathbf{b}$ is also from C. Let $*$ be a $\mathbf{F}_{p^t}$-bilinear form (an *inner product*). A code C is selforthogonal for $*$ if for all vectors $\mathbf{a}$ and $\mathbf{b}$ from C the following property holds

$$\mathbf{a} * \mathbf{b} = 0. \tag{1}$$

The code $C^{\perp} = \{\mathbf{v} : \mathbf{v} * \mathbf{a} = 0 \text{ for } \forall \mathbf{a} \in C\}$ is called dual of C with respect to (1).

Remark For an introduction to the theory of Galois Fields and classical codes see e.g. [14].

A q-ary quantum code Q of length n and size K is a K-dimensional subspace of a q^n-dimensional Hilbert space. This Hilbert space is identified with the n-fold tensor product of q-dimensional Hilbert spaces. The q-dimensional spaces are thought of as the state spaces of *q-ary systems* in the same way as the values 0 and 1 can be thought of as the possible states of a bit in a bit string. We identify the state spaces with the q-dimensional complex linear space $\mathbf{C}_q$. An important characteristic of a quantum code is its minimum distance. If a code has minimum distance d then it can detect any $d-1$ and correct any $\lfloor \frac{d-1}{2} \rfloor$ errors. As a result it is desirable to keep d as large as possible. A strict definition of the minimum distance is given in the next section after introducing error bases.

Remark For introductions to the theory of quantum error correcting codes see e.g. [12, 9, 13]. For a reader with a background in classical coding theory the papers [1, 2, 3] have brief introductions to the field.

3 Error Basis

A general quantum error of a p^m-ary quantum system, is a linear operator acting on the space $\mathbf{C}_{p^m}$. If $|\mathbf{v}\rangle$ is a state (a unit vector in the space) of the system, then the effect of error E is to transform it to the state $E|\mathbf{v}\rangle$. It is convenient to confine ourselves to errors that form a basis of the vector space of linear operators acting on $\mathbf{C}_{p^m}$. Let linear operators $e_1, e_2, \ldots, e_{p^{2m}}$ form such a basis. If $|\mathbf{v}\rangle$ represents a state of n p^m-ary systems it can be altered by an error operator of the form

$$E = \sigma_1 \otimes \sigma_2 \otimes \ldots \otimes \sigma_n, \tag{2}$$

where $\sigma_i \in \{e_1, e_2, \ldots, e_{p^{2m}}\}$. A general error operator is a linear operator acting on the n-fold tensor product of $\mathbf{C}_{p^m}$. Any such operator can be written down as a linear combination of error operators of the form (2). It is well known from the general theory of quantum codes that if a code can correct a given set $\mathcal{E}$ of error operators, then it can correct the linear span of $\mathcal{E}$. For this reason it makes sense to focus on operators of the form (2).

It is always possible to determine operators e_1, $e_2, \ldots, e_{p^{2m}}$ in such a way that one of them, say e_1, is the identity operator I_{p^m}. Define the *weight* of E in (2) as

$$\mathrm{wt}(E) = |\{\sigma_i \neq I_{p^m}\}|. \tag{3}$$

In the depolarizing channel model of errors [4], the operators $e_2, e_3, \ldots$ satisfy $\mathrm{Tr}(e_i^{\dagger} e_j) = p^m \delta_{i,j}$, where Tr is the trace of linear operators. When transmitting a qubit through a depolarizing channel, the probability that it is untouched (i.e. affected by the identity operator) is $1-r$ and the probability that it is affected by $e_i, i > 1$, is $r/(p^{2m}-1)$. Thus, the probability of an error operator decreases exponentially with weight, a feature common to most realistic error models [13]. This explains why it is desirable to correct or detect all error operators up to some given weight.

Let P be the orthogonal projection operator onto Q. It can be shown that (see e.g. [10]) an error operator E is detectable by Q iff

$$PEP = c_E P. \tag{4}$$

The largest integer d such that every error of weight $d-1$ or less can be detected by a code is called its minimum distance.

We now define an explicit error basis for p^m-ary quantum codes. Let T and R be linear operators acting on the space $\mathbf{C}_p$ defined by the matrices with entries

$$T_{i,j} = \delta_{i,j-1 \bmod p} \text{ and } R_{i,j} = \xi^i \delta_{i,j},$$

where $\xi = e^{\iota 2\pi/p}$, $\iota = \sqrt{-1}$ and the indices range from 0 to $p-1$ [10]. It is easy to check that

$$TR = \xi RT$$

and therefore

$$\begin{aligned} T^i R^j &= \xi^{ij} R^j T^i, & (5)\\ \left(T^i R^j\right)\left(T^k R^l\right) &= \xi^{il-jk}\left(T^k R^l\right)\left(T^i R^j\right), & (6)\\ \left(T^i R^j\right)\left(T^k R^l\right) &= \xi^{-jk} T^{i+k} R^{j+l}. & (7) \end{aligned}$$

The Hermitian transposes of T^i and R^i are obtained by raising to the power $p-1$:

$$(T^i)^{\dagger} = (T^i)^{p-1}, (R^i)^{\dagger} = (R^i)^{p-1}. \tag{8}$$

Note that

$$T^p = R^p = I_p. \tag{9}$$

From (7) and (9) it follows that for $p > 2$

$$(T^i R^j)^p = \xi^{-ij(1+2+\ldots+(p-1))} = I_p. \tag{10}$$

Since $\mathrm{Tr}(T^i R^j) = 0$ except when $i = j = 0 \bmod p$, the operators $T^i R^j$ form an orthogonal operator basis under the usual inner product for operators given by $\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$. Let $a, b \in \mathbf{F}_{p^m}$. Using a basis of $\mathbf{F}_{p^m}$ over $\mathbf{F}_p$, we can write uniquely

$$\begin{aligned} a &= a_1\alpha_1 + a_2\alpha_2 + \ldots + a_m\alpha_m, \\ b &= b_1\alpha_1 + b_2\alpha_2 + \ldots + b_m\alpha_m, \end{aligned}$$

with the a_i and b_i in $\mathbf{F}_p$. Define

$$T_a R_b = (T^{a_1} \otimes T^{a_2} \otimes \ldots \otimes T^{a_m})(R^{b_1} \otimes R^{b_2} \otimes \ldots \otimes R^{b_m}).$$

The operators $T_a R_b$ then form an orthonormal basis. The multiplication rules given above can be generalized. Define

$$\langle a, b\rangle = \sum_{i=1}^{m} a_i b_i \in \mathbf{F}_p. \tag{11}$$

From (7) and the identity $(A \otimes B)(C \otimes D) = AC \otimes BD$ it follows that

$$(T_a R_b)(T_c R_d) = \xi^{-\langle b,c\rangle} T_{a+c} R_{b+d}. \tag{12}$$

(6) and (11) yield

$$(T_a R_b)(T_c R_d) = \xi^{\langle a,d\rangle - \langle b,c\rangle}(T_c R_d)(T_a R_b). \tag{13}$$

4 Nonbinary Stabilizer Codes

Let $\mathbf{a}^\dagger = (a^{(1)}, a^{(2)}, \ldots, a^{(n)}), \mathbf{b}^\dagger = (b^{(1)}, b^{(2)}, \ldots, b^{(n)})$ be vectors from the space $\mathbf{F}_{p^m}^n$. (Throughout this section we use superscripts to label the systems.) As discussed in the previous section, it is enough to consider the error operators given by

$$E_{\mathbf{a},\mathbf{b}} = T_{a^{(1)}} R_{b^{(1)}} \otimes T_{a^{(2)}} R_{b^{(2)}} \otimes \ldots \otimes T_{a^{(n)}} R_{b^{(n)}}. \tag{14}$$

The set of operators $\mathcal{E} = \{\xi^i E_{\mathbf{a},\mathbf{b}} | 0 \le i \le p-1\}$ form a group of order p^{2mn+1}. The center $\mathcal{Z}$ of $\mathcal{E}$ is generated by ξI and therefore has order p. For vectors $\mathbf{a}, \mathbf{d} \in \mathbf{F}_{p^m}^n$ define an inner product by

$$\langle \mathbf{a}, \mathbf{d}\rangle = \sum_{i=1}^{n} \langle a^{(i)}, d^{(i)}\rangle, \tag{15}$$

where $\langle a^{(i)}, d^{(i)}\rangle$ is defined in (11). It follows from (13) that

$$E_{\mathbf{a},\mathbf{b}} E_{\mathbf{c},\mathbf{d}} = \xi^{\langle \mathbf{a},\mathbf{d}\rangle - \langle \mathbf{b},\mathbf{c}\rangle} E_{\mathbf{c},\mathbf{d}} E_{\mathbf{a},\mathbf{b}}. \tag{16}$$

From (12) we have

$$E_{\mathbf{a},\mathbf{b}} E_{\mathbf{c},\mathbf{d}} = \xi^{-\langle \mathbf{b},\mathbf{c}\rangle} E_{\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{d}}. \tag{17}$$

From (14) and (10) it follows that for any $\mathbf{a}$ and $\mathbf{b}$ and $p > 2$,

$$E_{\mathbf{a},\mathbf{b}}^p = I_{p^{mn}}. \tag{18}$$

Quantum *stabilizer codes* are defined as joint eigenspaces of the operators of a commutative subgroup S of $\mathcal{E}$. Without loss of generality, assume that $\mathcal{Z} \subseteq S$. If this is not the case, extend S by $\mathcal{Z}$. The order of S is a power of p, $|S| = p^{r+1}$. The joint eigenspaces of S are associated with linear characters μ of the group S whose value $\mu(E)$ is the eigenspace's eigenvalue with respect to E. Clearly it must be the case that $\mu(\xi I) = \xi$. Let μ be any one of the p^r characters of S which satisfy this constraint. We define a quantum stabilizer code Q as the eigenspace associated with μ. To determine the dimension of Q, consider the orthogonal projection operator P on Q, which can be written in the form

$$P = \frac{1}{|S|} \sum_{E \in S} \bar{\mu}(E) E.$$

Since for $E \in \mathcal{E} \setminus \mathcal{Z}$, $\mathrm{Tr}\, E = 0$, we have

$$\begin{aligned} \dim Q &= \mathrm{Tr}\, P \\ &= \frac{1}{|S|} \sum_{i=0}^{p-1} \bar{\mu}(\xi^i I)\, \mathrm{Tr}(\xi^i I) \\ &= \frac{1}{p^{r+1}} \sum_{i=0}^{p-1} p^{mn} \\ &= p^{mn-r}. \end{aligned}$$

Hence Q is an $[[n, mn-r]]_{p^m}$ quantum stabilizer code.

We next establish a connection between quantum stabilizer and classical selforthogonal codes. Note

that since the error basis is obtained as a tensor product of p-ary error bases, stabilizer codes can be viewed as standard p-ary stabilizer codes. This situation is essentially the same as for classical linear codes over $\mathbf{F}_{p^m}$. However, since the goal is to protect against errors on p^m-ary systems, we wish to usefully relate p^m-ary stabilizer codes to classical codes over $\mathbf{F}_{p^{2m}}$.

First we show how to construct a classical code from a quantum code. Let φ be an isomorphism of the vector space $\mathbf{F}_p^m$. Clearly the set $C = \{(\mathbf{a}, \varphi^{-1}\mathbf{b}) | E_{\mathbf{a},\mathbf{b}} \in S\}$ is an $\mathbf{F}_p$-linear code of length $2n$ and size p^r. Moreover, since all operators from S commute the following property holds for any two vectors $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{a}', \mathbf{b}')$ from C

$$\langle \mathbf{a}, \varphi(\mathbf{b}') \rangle - \langle \mathbf{a}', \varphi(\mathbf{b}) \rangle = 0. \tag{19}$$

Thus C is selforthogonal with respect to the inner product defined by $(\mathbf{a}, \mathbf{b}) * (\mathbf{a}', \mathbf{b}') = \langle \mathbf{a}, \varphi(\mathbf{b}') \rangle - \langle \mathbf{a}', \varphi(\mathbf{b}) \rangle$. Later we will choose φ to relate the inner product to the structure of $\mathbf{F}_{p^m}$.

The minimum distance of a stabilizer code defined by S is related to the classical minimum distance of $C^\perp \setminus C$, where $C^\perp$ is the dual code of C with respect to (19). Define the weight of $\mathbf{v} = (\mathbf{a}, \mathbf{b}) \in \mathbf{F}_{p^m}^{2n}$ as

$$\mathrm{wt}(\mathbf{v}) = |\{i : a^{(i)} \neq 0 \text{ or } b^{(i)} \neq 0\}|.$$

Using arguments similar to ones from [6], one can show that the minimum distance of a stabilizer code of S equals $\min\{\mathrm{wt}(\mathbf{v}) : \mathbf{v} \in C^\perp \setminus C\}$. For completeness we give a general proof of this fact.

Denote by $S^\perp$ the group of operators in $\mathcal{E}$ that commute with all operators from S. Thus $S^\perp$ is given by $S^\perp = \{\xi^i E_{\mathbf{a},\mathbf{b}} : (\mathbf{a}, \mathbf{b}) \in C^\perp\}$. The desired fact follows from the observation that $E' \in \mathcal{E}$ is detectable iff $E' \notin S^\perp \setminus S$. Let P be as defined earlier. We consider three cases.

1. Let $E' \in S$. Then

$$\begin{aligned} E'P &= \frac{1}{|S|} \sum_{E \in S} \bar{\mu}(E) E'E \\ &= \frac{1}{|S|} \sum_{E \in S} \bar{\mu}((E')^\dagger E) E \\ &= \mu(E') P, \end{aligned} \tag{20}$$

   where the last equality follows from linearity of μ. Thus

$$PE'P = \mu(E')P$$

   and hence E' is detectable.

2. Let $E' \notin S^\perp$. Let S_i, $0 \leq i < p$, be defined by $S_i = \{E \in S : E'E = \xi^i E E'\}$. Then from (16) and the assumption, it follows that $|S_i| = |S|/p$. Thus

$$\begin{aligned} |S|PE'P &= \sum_{E \in S} \bar{\mu}(E) E E' P \\ &= E' \sum_{i=0}^{p-1} \sum_{E \in S_i} \xi^i \bar{\mu}(E) E P \\ &= E' \sum_{i=0}^{p-1} \sum_{E \in S_i} \xi^i P \\ &= E' \sum_{i=0}^{p-1} \xi^i P |S|/p \qquad (21) \\ &= 0, \qquad (22) \end{aligned}$$

   where we used (20) in the third to last step. Again, E' is detectable.

3. Let $E' \in S^\perp \setminus S$. By taking T to be the commutative subgroup generated by S and E' and extending the character μ to T, a subcode Q' of Q is obtained corresponding to the extended character. The dimension of Q' is smaller by a factor of p, which implies that Q is not an eigenspace of E'. Since E' commutes with S, E' preserves Q. All of this implies that $PE'P$ is not proportional to P.

The inner product defined in (19) depends on the isomorphism φ. Clearly, the set of codes obtained does not depend on φ, so the choice of φ is primarily one of convenience. We now standardize this choice to simplify the construction of large minimum distance codes. With respect to our distinguished basis of $\mathbf{F}_{p^m}$, φ is given by an $m \times m$ matrix M over $\mathbf{F}_p$. Choose M by defining

$$M_{i,j} = \mathrm{tr}(\alpha_i \alpha_j).$$

With $a^T = (a_1, a_2, \ldots, a_m), b^T = (b_1, b_2, \ldots, b_m) \in \mathbf{F}_{p^m}$, we compute

$$\begin{aligned} a^T M b &= \sum_{i=1}^m \sum_{j=1}^m a_i b_j \,\mathrm{tr}(\alpha_i \alpha_j) \\ &= \sum_{i=1}^m \sum_{j=1}^m \mathrm{tr}(a_i b_j \alpha_i \alpha_j) \\ &= \mathrm{tr}\left(\left(\sum_{i=1}^m a_i \alpha_i \right) \left(\sum_{i=1}^m b_i \alpha_i \right) \right) \\ &= \mathrm{tr}(ab), \end{aligned}$$

where the product in the trace is multiplication in $\mathbf{F}_{p^m}$. For vectors $\mathbf{a}$ and $\mathbf{b}$ in $\mathbf{F}_{p^m}^n$, let $\langle \mathbf{a}, \mathbf{b} \rangle_* = \sum_i a^{(i)} b^{(i)}$. With this choice of φ, C is therefore selforthogonal with respect to the inner product defined by

$$(\mathbf{a}, \mathbf{b}) * (\mathbf{a}', \mathbf{b}') = \operatorname{tr}(\langle \mathbf{a}, \mathbf{b}' \rangle_* - \langle \mathbf{a}', \mathbf{b} \rangle_*). \tag{23}$$

We can now construct a quantum stabilizer code from a classical selforthogonal code $C, |C| = p^r$. Let vectors $\mathbf{v}_i = (\mathbf{a}_i, \mathbf{b}_i), 0 \le i \le r-1$ form a basis of C over $\mathbf{F}_p$. Then the p^r operators $E_{\mathbf{a}_i, \phi(\mathbf{b}_i)}$ together with $\xi I_{p^{mn}}$ generate a group of commuting operators of order p^{r+1}, which defines $[[n, mn-r]]_{p^m}$ stabilizer codes with minimum distance $d = \min\{\mathrm{wt}(\mathbf{v}) : \mathbf{v} \in C^\perp \setminus C\}$.

In [5] a number of families of good classical codes that are selforthogonal with respect to the inner product

$$(\mathbf{a}, \mathbf{b}) * (\mathbf{a}', \mathbf{b}') = \langle \mathbf{a}, \mathbf{b}' \rangle_* - \langle \mathbf{a}', \mathbf{b} \rangle_* \tag{24}$$

where constructed. Since a code that is selforthogonal with respect to (24) is also selforthogonal with respect to (23), our results establish a previously missing connection between the classical codes defined in [5] and quantum codes. Thus we already have many good nonbinary stabilizer codes. For instance from [5] we can obtain quantum stabilizer codes with parameters $[[q^r, q^r - (r+2), 3]]_q$, $[[q^2+1, q^2-3, 3]]_q$, $[[(q^{r+2}-1)/(q^2-1), (q^{r+2}-1)/(q^2-1) - (r+2), 3]]_q$ (r is even) , $[[q^3(q^{r-1}-1)/(q^2-1), q^3(q^{r-1}-1)/(q^2-1) - (r+2), 3]]_q$ (r is odd) , and others.

In conclusion, we note that if a code is $\mathbf{F}_{p^m}$-linear and is selforthogonal with respect to (23) then it is automatically selforthogonal with respect to (24). Since this does not hold for general $\mathbf{F}_p$-linear codes, one expects to find better codes selforthogonal with respect to (23) in this class.

Acknowledgements. E. K. was supported by funding from NSA and DOE.

References

[1] A. Ashikhmin and S. Litsyn, "Upper bounds of the size of quantum codes," *IEEE Trans. Info. Theory*, vol 45, no. 4, pp.1205-1215, 1999.

[2] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn, "Quantum Error Detection I: Statement of the Problem ," *IEEE Trans. Info. Theory*, to appear .

[3] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn, "Quantum Error Detection II: Bounds ," *IEEE Trans. Info. Theory*, to appear .

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, "Mixed state entanglement and quantum error-correcting codes," *Phys. Rev. A*, vol. 54, pp. 3824–, 1996.

[5] J. Bierbrauer and Y. Edel, "Quantum Twisted Codes," *preprint*, 1998. (The paper is available at "http://www.math.mtu.edu∼jbierbra/".)

[6] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405-409, 1997.

[7] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum errors correction via codes over $GF(4)$,"*IEEE Trans. Info. Theory*, vol. 44, pp.1369 –1387, 1998.

[8] D. Gottesman, "A class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol.54, pp. 1862-1868, 1996.

[9] D. Gottesman, "Stabilizer Codes and Quantum Error Correction," *Ph.D. Thesis,* California Institute of Technology, Pasadena, California, 1997.

[10] E. Knill, "Non-binary Unitary Error Bases and Quantum Codes," *LANL Preprint*, quant-ph/9608048, 1996.

[11] E. Knill, "Group Representations, Error Bases and Quantum Codes," *LANL Preprint*, quant-ph/9608049, 1996.

[12] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Phys. Rev. A*, vol. 55, pp. 900-911, 1997.

[13] E. Knill, R. Laflamme and L. Viola, "Theory of quantum error correction for general noise", *Phys. Rev. Lett.*, vol. 84, pp. 2525-2528, 2000.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland, 1977.

[15] E. Rains, Nonbinary quantum codes, LANL e-print quant-ph/9703048.

[16] P.W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, S.Goldwasser, Editor, IEEE Computer Society Press, Los Alamitos, CA, p.124, 1994.

[17] P.W. Shor, “Scheme for reducing decoherence in quantum memory,” Phys. Rev. A, **52**, p. 2493, 1995.

[18] P.W. Shor and R. Laflamme, “Quantum analog of the MacWilliams identities in classical coding theory,” *Phys. Rev. Lett.*, vol. 78, pp. 1600-1602, 1997.

[19] A. M. Steane, ”Simple quantum error correcting codes,” *Phys. Rev. Lett.*,vol. 77, pp. 793-797, 1996.

[20] A. M. Steane, ”Multiple particle interference and quantum error correction,” *Proc. Roy. Soc. London A*, vol. 452, pp. 2551-2577, 1996.